Deutscher Bundestag **Drucksache 17/6293**

17. Wahlperiode 28. 06. 2011

Antrag

der Abgeordneten Wolfgang Gunkel, Heinz-Joachim Barchmann, Gabriele Fograscher, Petra Ernstberger, Iris Gleicke, Kerstin Griese, Michael Hartmann (Wackernheim), Dr. Eva Högl, Frank Hofmann (Volkach), Daniela Kolbe (Leipzig), Ute Kumpf, Christine Lambrecht, Kirsten Lühmann, Dietmar Nietan, Thomas Oppermann, Gerold Reichenbach, Michael Roth (Heringen), Werner Schieder (Weiden), Dr. Martin Schwanholz, Peer Steinbrück, Rüdiger Veit, Dr. Dieter Wiefelspütz, Dr. Frank-Walter Steinmeier und der Fraktion der SPD

Übermittlung von Fluggastdaten nur nach europäischen Grundrechts- und Datenschutzmaßstäben

hier: Stellungnahme gegenüber der Bundesregierung gemäß Artikel 23 Absatz 3 des Grundgesetzes i. V. m. § 9 Absatz 4 EUZBBG zum Richtlinienvorschlag KOM(2011) 32 endg.

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Am 2. Februar 2011 hat die Europäische Kommission einen Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität vorgelegt (KOM(2011) 32 endg.).

Der Entwurf muss datenschutzrechtlich erheblich verbessert werden. Zwar verfolgt er ein legitimes Anliegen. Die Mitgliedstaaten der Europäischen Union müssen terroristische und strafrechtliche Bedrohungen abwehren. Doch müssen sie dabei die grund- und menschenrechtlichen Garantien beachten, die zu den Rechtstraditionen der Mitgliedstaaten zählen und in der Grundrechtecharta der Europäischen Union verankert sind. Dies ist durch die im Entwurf vorgesehenen Regelungen noch nicht ausreichend gewährleistet. Insbesondere müssen die nachfolgenden datenschutzrechtlichen Gesichtspunkte dringend nachverhandelt werden.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

bei den weiteren Verhandlungen über den Richtlinienvorschlag im Rat folgende Maßstäbe als wesentliche Belange im Sinne von § 9 Absatz 4 des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union (EUZBBG) durchzusetzen:

1. Die Richtlinie soll einen wirksamen Beitrag zum Schutz vor schwerer Kriminalität und Terrorismus leisten. Gleichzeitig muss sie den effektiven Schutz

personenbezogener Daten gewährleisten, wie er in Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union, den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union, Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, im Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und im europäischen Sekundärrecht garantiert ist.

2. Die Maßstäbe des deutschen Datenschutzes, wie sie vom Bundesverfassungsgericht (BVerfG) zum Recht auf informationelle Selbstbestimmung konkretisiert worden sind, sind in die Richtlinie aufzunehmen. Das gilt insbesondere für die Grundsätze zur so genannten Vorratsdatenspeicherung.

3. Die Erhebung, Verarbeitung und Nutzung müssen geeignet, erforderlich und angemessen sein. Das bedeutet insbesondere, dass folgende Anforderungen in der Richtlinie zu verankern sind:

   a) Art und Umfang der erhobenen Daten müssen genau und abschließend begrenzt werden. Vorbild für die zu erhebenden Daten soll Artikel 3 Absatz 2 der Richtlinie 2004/82/EG sein, der in § 31a des Bundespolizeigesetzes (BPolG) umgesetzt worden ist.

   b) Die bislang vorgesehene Speicherfrist ist auf deutlich unter sechs Monate zu begrenzen.

   c) Es darf keine Ermächtigung zum automatisierten Datenabgleich geschaffen werden.

   d) Der Abruf und die Nutzung der Daten dürfen nur bei einem durch bestimmte Tatsachen begründeten Verdacht auf schwere oder terroristische Straftaten erfolgen.

   e) Der Abruf und die Nutzung der Daten sind dem Richtervorbehalt zu unterlegen.

   f) Es ist klarzustellen, dass die Beantwortung individueller Anfragen der zuständigen Sicherheitsbehörden anhand des so genannten Push-Systems zu erfolgen hat. Bei diesem hat die anfragende Behörde keinen direkten Zugriff auf die Daten. Vielmehr werden ihr diese auf Anfrage von der speichernden Behörde übermittelt.

   g) Es ist auf ausreichende Bestimmungen zum technischen Datenschutz hinzuwirken. Dazu gehören neben der Verwendung gemeinsamer Protokolle namentlich die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung. Eine effektive Kontrolle muss gewährleistet werden, Verstöße müssen wirksam sanktioniert werden.

   h) Die Weitergabe der Daten an Drittstaaten ist nur zulässig, sofern dies in internationalen Abkommen, die ein ausreichendes Datenschutzniveau gewährleisten, vorgesehen ist.

   i) Der Anwendungsbereich der Richtlinie darf nicht auf innereuropäische Flüge sowie auf andere Verkehrsmittel als Flugzeuge ausgeweitet werden.

   j) Es darf im Laufe der weiteren Verhandlungen nicht hinter bereits im Richtlinien-Vorschlag enthaltene datenschutzrechtliche Maßstäbe zurückgefallen werden. Das gilt insbesondere für

      - die Beibehaltung der in Artikel 2 Buchstabe g, h und i des Richtlinienentwurfs enthaltenen Beschränkung auf terroristische und schwere Straftaten i. S. d. dort genannten Normen der Rahmenbeschlüsse 2002/475/JI und 2002/584/JI des Rates,

- die Beibehaltung der in Artikel 11 Absatz 1 des Richtlinienentwurfs vorgesehene Gewährleistung ausreichender Auskunft, Berichtigung, Löschung und Sperrung, Schadenersatz und Rechtsbehelfe,
- die Beibehaltung der in Artikel 11 Absatz 4 vorgesehenen Protokollierung sowie
- die Beibehaltung des so genannten Push-Systems zwischen Fluglinien und PNR-Zentralbehörde (Passenger Name Record) (Artikel 6 Absatz 1 des Richtlinienentwurfs).

Berlin, den 28. Juni 2011

Dr. Frank-Walter Steinmeier und Fraktion

Begründung

Zu Nummer 1

Die Forderung soll gewährleisten, dass eine ausreichende Abwägung zwischen Sicherheitsbedürfnissen und Grundrechtsschutz in der Richtlinie zum Ausdruck kommt.

Zu Nummer 2

Das BVerfG hat im Urteil vom 2. März 2010 (1 BvR 256/08) hohe Anforderungen an die so genannte Vorratsdatenspeicherung gestellt. Hierzu zählt das Gericht die Datenspeicherung „ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation. Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist“ (BVerfG a. a. O. Rn. 210). Diese Definition trifft auf die Speicherung von PNR-Daten zu. Sie werden allein deshalb erhoben, weil Reisende das Flugzeug wählen, also ein sozial ebenso gebilligtes wie unverzichtbares Alltagshandeln an den Tag legen.

Zwar ist deutsches Verfassungsrecht gemeinschaftsrechtlich für die Wirksamkeit der Richtlinie unbeachtlich. Politisch ist eine am Urteil des BVerfG ausgerichtete Verhandlungsführung dennoch aus zwei Gründen geboten. Erstens ist es erstrebenswert, die im europäischen Vergleich hohen datenschutzrechtlichen deutschen Maßstäbe auf die europäische Ebene zu übertragen, um zur Vertiefung des Datenschutzes im europäischen Sekundärrecht beizutragen. Zweitens ist es integrationspolitisch erforderlich, einen Konflikt zwischen Gemeinschaftsrecht und nationalem Verfassungsrecht zu vermeiden.

Zu Nummer 3 Buchstabe a

Aus der Rechtsprechung des BVerfG ergeben sich auch im Hinblick auf den Umfang der abzurufenden Daten verfassungsrechtliche Grenzen (BVerfG a. a. O. Rn. 237). Die laut Anhang zum Richtlinienentwurf RL-E erhobenen Daten sind jedoch sehr umfangreich. Mit 19 Kategorien sind sie umfänglicher als die nach Artikel 3 Absatz 2 der Richtlinie 2004/82/EG erhobenen Daten, die so genannten API-Daten (Advance Passenger Information). Letztere enthalten einen abschließenden und bestimmten Datenkatalog. Sie werden, dem Ziel der Richtlinie 2004/82/EG folgend, zur Bekämpfung der illegalen Einreise erhoben. Aus der bundespolizeilichen Praxis werden keine Fälle berichtet, in denen dieser Datenbestand als nicht ausreichend erachtet wurde.

Auch die Europäische Kommission hat nicht ausreichend begründet, warum dieser Datenbestand ungenügend sein soll. Zwar erlaubten es die API-Daten der Kommission zufolge nicht, „‚unbekannte‘ Verdächtige so zu identifizieren wie dies mit einer Auswertung von PNR-Daten möglich ist“ (KOM(2011) 32 endg., S. 5). Diese Aussage wird jedoch nicht näher belegt. Deshalb teilt der Deutsche Bundestag die Auffassung des Bundesrates: „Diese pauschale Aussage kann nicht als ausreichend angesehen werden. Soweit ersichtlich, ist bislang nicht ausreichend untersucht worden, wie die vorhandenen Instrumente zur Bekämpfung des Terrorismus und der schweren Kriminalität nutzbar gemacht werden könnten“ (Bundesratsdrucksache 73/11 (Beschluss), S. 3).

Zu Nummer 3 Buchstabe b

Nach dem BVerfG ist die anlasslose Datenspeicherung unter bestimmten Voraussetzungen bis zu einer Höchstdauer von sechs Monaten zulässig (BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08 Rn. 215). Die bisher bekannt gewordenen Ergebnisse der auf europäischer Ebene erfolgten Evaluierung haben ergeben, dass eine Speicherfrist von sechs Monaten zur Strafverfolgung nicht erforderlich ist. Circa 70 Prozent der Abfragen von Daten erfolgen in den ersten drei Monaten; der Anteil steigt auf 85 Prozent, wenn die Daten maximal sechs Monate alt sind. Dieses Ergebnis deckt sich mit den Erfahrungen auf nationaler Ebene.

Die bislang vorgesehene Speicherung von fünf Jahren und 30 Tagen ist zu lang. Zwar werden die vollständig sichtbaren Daten gemäß Artikel 9 Absatz 2 Satz 1 und 2 des Richtlinienentwurfs zunächst nur für 30 Tage gespeichert. Gemäß Absatz 2 derselben Norm folgt aber eine Speicherung von weiteren fünf Jahren. Zwar wird diese in Artikel 9 Absatz 2 Satz 3 des Richtlinienentwurfs als anonymisierte Speicherung bezeichnet, weil die Identitätsdaten gemäß Satz 2 der genannten Norm nicht sichtbar sein dürfen. Gemäß Artikel 9 Absatz 2 Satz 4 RL-E ist jedoch der Zugriff unter den dort genannten Voraussetzungen auf die vollständigen Daten nach wie vor möglich. Der Deutsche Bundestag teilt deshalb die vom Bundesrat vertretene Auffassung, dass es sich hierbei nur um eine scheinbare Anonymisierung handelt (Bundesratsdrucksache 73/11 (Beschluss), S. 3).

Zu Nummer 3 Buchstabe c

Nach der Rechtsprechung des BVerfG zur so genannten Rasterfahndung ist ein automatisierter Datenabgleich (Rasterung) mit dem Grundrecht auf informationelle Selbstbestimmung nur dann vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr hingegen scheidet eine solche Rasterfahndung aus (BVerfG, Urteil vom 4. April 2006, 1 BvR 518/02, Leitsatz 1 und Rn. 125 ff.).

Der RL-E sieht jedoch eine solche anlasslose Rasterung im Vorfeld der Gefahrenabwehr vor. Artikel 4 Absatz 2 Buchstabe a und b RL-E ermächtigen die PNR-Zentralstellen dazu, PNR-Daten anhand im Voraus festgelegter Kriterien im automatisierten Verfahren zu überprüfen. Sofern sich Treffer ergeben, sind diese Treffer den eben genannten Normen zufolge auf andere, nichtautomatisierte Weise an die zuständigen Ermittlungsbehörden zu ermitteln.

Weiterhin ermächtigt Artikel 4 Absatz 2 Buchstabe d RL-E zur Auswertung von verdachtslos erhobenen PNR-Daten zwecks Aktualisierung oder Aufstellung neuer Kriterien für die Durchführung von individuellen Überprüfungen von Fluggästen. Ausweislich der Begründung dient dies dem Ziel, „Personen zu identifizieren, die ihnen bislang nicht ‚bekannt‘ waren, d. h. Personen, die noch nicht im Verdacht stehen, an einer (…) Straftat beteiligt zu sein, bei denen eine Datenauswertung aber Anhaltspunkte dafür liefert, dass sie an einer solchen

Straftat beteiligt sein könnten (…)“. Dazu müsse anhand zuvor festgelegter Prüfkriterien ein Abgleich vorgenommen werden (KOM(2011) 32 endg., S. 5).

Damit liegt eine nach der Rechtsprechung des BVerfG unzulässige Ermächtigung zur Rasterfahndung vor. Die entsprechende Norm gibt auch keinen Umsetzungsspielraum für eine grundgesetzkonforme innerstaatliche Umsetzung. Denn der Wortlaut ist nicht nur als Ermächtigung, sondern gleichzeitig als Verpflichtung der zentralen PNR-Behörde zur entsprechenden Datenverarbeitung zu lesen (vgl. Artikel 3 Absatz 1 i. V. m. Artikel 4 Absatz 2 RL-E). Folglich wäre eine verfassungskonforme Umsetzung des bisher vorgesehenen Artikels 4 Absatz 2 Buchstabe a, b und d RL-E nicht möglich.

Zu Nummer 3 Buchstabe d

Diese Beschränkung dient der Wahrung der Verhältnismäßigkeit. Sie setzt die vom BVerfG zur Vorratsdatenspeicherung geforderte hohe Eingriffsschwelle um (vgl. BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08, Leitsatz 5 und Rn. 228).

Zu Nummer 3 Buchstabe e

Diese Beschränkung dient der Wahrung der Verhältnismäßigkeit. Sie setzt die vom BVerfG zur Vorratsdatenspeicherung geforderte Gewährleistung eines effektiven Rechtsschutzes um (vgl. BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08, Rn. 247).

Zu Nummer 3 Buchstabe f

Die Formulierung in Artikel 4 Absatz 2 Buchstabe d RL-E, der die Beantwortung von individuellen Anfragen von Sicherheitsbehörden regelt, legt nahe, dass ein Push-System gemeint ist. Anders als in Artikel 6 Absatz 1 RL-E, der die Übermittlung zwischen Fluglinien und PNR-Zentralstelle regelt, ist dies jedoch nicht ausdrücklich klargestellt.

Zu Nummer 3 Buchstabe g

Der technische Datenschutz ist teilweise durch den in Artikel 11 Absatz 2 RL-E enthaltenen Verweis auf die Artikel 21 und 22 des Rahmenbeschlusses 2008/977/JI des Rates sowie die in Artikel 11 Absatz 4 RL-E vorgeschriebene Protokollierung und Dokumentation gewährleistet. Die darin enthaltenen Vorgaben sind jedoch nicht ausreichend.

Insbesondere ist keine spezielle Pflicht zur Verschlüsselung enthalten. Artikel 13 Absatz 2 RL-E schreibt nur die Verwendung gemeinsamer Protokolle vor. Diese stellen lediglich einen geschützten Übermittlungsweg bzw. -kanal dar. Daneben ist zu fordern, auch die darin übermittelten Datensätze selbst zu verschlüsseln. Nur so sind diese Daten auch dann geschützt, wenn sich Unbefugte Zugriff auf die gemeinsamen Protokolle verschaffen.

Zudem erlaubt Artikel 6 Absatz 2 RL-E im Falle technischer Störungen eine Übermittlung auf „jede sonstige geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet.“ Dies ist eine zu weite und unbestimmte Öffnungsklausel.

Zu Nummer 3 Buchstabe h

Artikel 8 RL-E erlaubt die Weitergabe der Daten an Drittstaaten. Neben anderen Voraussetzungen müssen sich diese bereit erklären, die Daten ausschließlich zu den im RL-E vorgesehenen Zwecken zu nutzen. Darüber hinaus ist eine Weitergabe an einen weiteren Drittstaat durch den Drittstaat möglich, sofern der übermittelnde Mitgliedstaat zustimmt. Diese Ermächtigung ist ebenso unbestimmt wie weitreichend.

Zu Nummer 3 Buchstabe i

Aus einzelnen Mitgliedstaaten wurde die Ausweitung des Anwendungsbereichs der Richtlinie auf innereuropäische Flüge sowie auf andere Verkehrsmittel als Flugzeuge gefordert. Bezüglich innereuropäischer Flüge befindet sich bereits ein entsprechender Prüfauftrag in Artikel 17 Buchstabe a RL-E. Dies ist in Bezug auf innereuropäische Flüge als unverhältnismäßige Einschränkung der gemeinschaftsrechtlichen Freizügigkeit abzulehnen. In Bezug auf die Ausweitung auf andere Verkehrsmittel als Flugzeuge ist dies als ebenso unverhältnismäßig wie unpraktikabel abzulehnen.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333